```
0
0x080484f0   push ebp
0x080484f1   mov ebp, esp
0x080484f3   push ebx
0x080484f4   push esi
0x080484f5   sub esp, 0x1a0
0x080484fb   mov eax, dword ptr [ebp+0xc]
0x080484fe   mov ecx, dword ptr [ebp+0x8]
0x08048501   lea edx, ptr [0x804ab08]
0x08048507   lea esi, ptr [ebp-0xb8]
0x0804850d   mov dword ptr [ebp-0xc], ecx
0x08048510   mov dword ptr [ebp-0x10], eax
0x08048513   mov dword ptr [ebp-0xbc], esi
0x08048519   mov dword ptr [ebp-0xf4], edx
```

```
1
0x0804851f   mov eax, dword ptr [ebp-0xf4]
0x08048525   movzx eax, byte ptr [eax]
0x08048528   mov ecx, eax
0x0804852a   sub ecx, 0x23
0x0804852d   mov dword ptr [ebp-0xf8], eax
0x08048533   mov dword ptr [ebp-0xfc], ecx
0x08048539   jnle 0x80485c6
```

```
2
0x0804853f   jmp 0x8048544
0x08048544   mov eax, dword ptr [ebp-0xf8]
0x0804854a   sub eax, 0x6
0x0804854d   mov dword ptr [ebp-0x100], eax
0x08048553   jnle 0x8048592
```

```
3
0x080485c6   mov eax, dword ptr [ebp-0xf8]
0x080485cc   sub eax, 0x59
0x080485cf   mov dword ptr [ebp-0x114], eax
0x080485d5   jnle 0x80486b0
```

```
4
0x08048559   jmp 0x804855e
0x0804855e   mov eax, dword ptr [ebp-0xf8]
0x08048564   sub eax, 0x2
0x08048567   mov dword ptr [ebp-0x104], eax
0x0804856d   jz 0x80490b4
```

```
5
0x08048592   mov eax, dword ptr [ebp-0xf8]
0x08048598   sub eax, 0x7
0x0804859b   mov dword ptr [ebp-0x10c], eax
0x080485a1   jz 0x8048e4c
```

```
6
0x080485db   jmp 0x80485e0
0x080485e0   mov eax, dword ptr [ebp-0xf8]
0x080485e6   sub eax, 0x33
0x080485e9   mov dword ptr [ebp-0x118], eax
0x080485ef   jnle 0x804862e
```

```
7
0x080486b0   mov eax, dword ptr [ebp-0xf8]
0x080486b6   sub eax, 0x94
0x080486bb   mov dword ptr [ebp-0x138], eax
0x080486c1   jnle 0x804874e
```

```
8
0x08048573   jmp 0x8048578
0x08048578   mov eax, dword ptr [ebp-0xf8]
0x0804857e   sub eax, 0x5
0x08048581   mov dword ptr [ebp-0x108], eax
0x08048587   jz 0x8048bf9
0x08048bf9   mov eax, dword ptr [ebp-0xf4]
0x08048bff   mov ecx, eax
0x08048c01   inc ecx
0x08048c02   mov dword ptr [ebp-0xf4], ecx
0x08048c08   mov eax, dword ptr [eax+0x5]
0x08048c0b   test eax, eax
0x08048c0d   mov dword ptr [ebp-0x188], eax
0x08048c13   jz 0x8048c4f
```

```
9
0x080490b4   mov eax, dword ptr [ebp-0xf4]
0x080490ba   add eax, 0x1
0x080490bd   mov dword ptr [ebp-0xf4], eax
0x080490c3   mov eax, dword ptr [ebp-0xbc]
0x080490c9   mov eax, dword ptr [eax]
0x080490cb   mov ecx, dword ptr [ebp-0xf4]
0x080490d1   mov ecx, dword ptr [ecx]
0x080490d3   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080490da   mov eax, dword ptr [ebp-0xf4]
0x080490e0   mov eax, dword ptr [eax+0x8]
0x080490e3   mov eax, dword ptr [ebp+eax*4-0xf0]
0x080490ea   mov ecx, dword ptr [ebp-0xf4]
0x080490f0   mov ecx, dword ptr [ecx+0x4]
0x080490f3   imul eax, dword ptr [ebp+ecx*4-0xf0]
0x080490fb   mov ecx, dword ptr [ebp-0xf4]
0x08049101   mov ecx, dword ptr [ecx+0xc]
0x08049104   mov dword ptr [ebp+ecx*4-0xf0], eax
0x0804910b   mov eax, dword ptr [ebp-0xbc]
0x08049111   mov eax, dword ptr [eax-0x4]
0x08049114   mov ecx, dword ptr [ebp-0xf4]
0x0804911a   mov ecx, dword ptr [ecx+0x10]
0x0804911d   mov ecx, dword ptr [ebp+ecx*4-0xf0]
0x08049124   mov eax, dword ptr [eax+ecx*1]
0x08049127   mov ecx, dword ptr [ebp-0xf4]
0x0804912d   mov ecx, dword ptr [ecx+0x14]
0x08049130   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049137   mov eax, dword ptr [ebp-0xf4]
0x0804913d   mov eax, dword ptr [eax+0x18]
0x08049140   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049147   mov ecx, dword ptr [ebp-0xbc]
0x0804914d   mov ecx, dword ptr [ecx-0x8]
0x08049150   mov dword ptr [ecx], eax
0x08049152   mov eax, dword ptr [ebp-0xf4]
0x08049158   mov eax, dword ptr [eax+0x24]
0x0804915b   mov ecx, dword ptr [ebp-0xf4]
0x08049161   mov ecx, dword ptr [ecx+0x20]
0x08049164   mov dword ptr [ebp+ecx*4-0xf0], eax
0x0804916b   mov eax, dword ptr [ebp-0xf4]
0x08049171   mov eax, dword ptr [eax+0x1c]
0x08049174   mov eax, dword ptr [ebp+eax*1-0x34]
0x08049178   mov ecx, dword ptr [ebp-0xf4]
0x0804917e   mov ecx, dword ptr [ecx+0x28]
0x08049181   add eax, dword ptr [ebp+ecx*4-0xf0]
0x08049188   mov ecx, dword ptr [ebp-0xf4]
0x0804918e   mov ecx, dword ptr [ecx+0x2c]
0x08049191   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049198   mov eax, dword ptr [ebp-0xbc]
0x0804919e   add eax, 0xfffffff4
0x080491a1   mov dword ptr [ebp-0xbc], eax
0x080491a7   mov eax, dword ptr [ebp-0xf4]
0x080491ad   add eax, 0x30
0x080491b0   mov dword ptr [ebp-0xf4], eax
0x080491b6   jmp 0x8049762
```

```
10
0x080485a7   jmp 0x80485ac
0x080485ac   mov eax, dword ptr [ebp-0xf8]
0x080485b2   sub eax, 0xc
0x080485b5   mov dword ptr [ebp-0x110], eax
0x080485bb   jz 0x8048a5f
0x08048a5f   lea eax, ptr [ebp-0x34]
0x08048a62   mov ecx, dword ptr [ebp-0xf4]
0x08048a68   add ecx, 0x1
0x08048a6b   mov dword ptr [ebp-0xf4], ecx
0x08048a71   mov ecx, dword ptr [ebp-0xf4]
0x08048a77   mov ecx, dword ptr [ecx+0x4]
0x08048a7a   mov edx, dword ptr [ebp-0xf4]
0x08048a80   mov edx, dword ptr [edx]
0x08048a82   mov dword ptr [ebp+edx*4-0xf0], ecx
0x08048a89   mov ecx, dword ptr [ebp-0xf4]
0x08048a8f   mov edx, eax
0x08048a91   add edx, dword ptr [ecx+0x8]
0x08048a94   mov ecx, dword ptr [ebp-0xf4]
0x08048a9a   mov ecx, dword ptr [ecx+0xc]
0x08048a9d   mov dword ptr [ebp+ecx*4-0xf0], edx
0x08048aa4   mov ecx, dword ptr [ebp-0xf4]
0x08048aaa   mov ecx, dword ptr [ecx+0x10]
0x08048aad   mov ecx, dword ptr [ebp+ecx*4-0xf0]
0x08048ab4   mov ecx, dword ptr [ecx]
0x08048ab6   mov edx, dword ptr [ebp-0xf4]
0x08048abc   mov edx, dword ptr [edx+0x14]
0x08048abf   mov dword ptr [ebp+edx*4-0xf0], ecx
0x08048ac6   mov ecx, dword ptr [ebp-0xf4]
0x08048acc   mov ecx, dword ptr [ecx+0x18]
0x08048acf   mov ecx, dword ptr [ebp+ecx*4-0xf0]
0x08048ad6   mov edx, dword ptr [ebp-0xf4]
0x08048adc   mov edx, dword ptr [edx+0x1c]
0x08048adf   add ecx, dword ptr [ebp+edx*4-0xf0]
0x08048ae6   mov edx, dword ptr [ebp-0xf4]
0x08048aec   mov edx, dword ptr [edx+0x20]
0x08048aef   mov dword ptr [ebp+edx*4-0xf0], ecx
0x08048af6   mov ecx, dword ptr [ebp-0xf4]
0x08048afc   add eax, dword ptr [ecx+0x28]
0x08048aff   mov ecx, dword ptr [ebp-0xf4]
0x08048b05   mov ecx, dword ptr [ecx+0x2c]
0x08048b08   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048b0f   mov eax, dword ptr [ebp-0xf4]
0x08048b15   mov eax, dword ptr [eax+0x24]
0x08048b18   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048b1f   mov ecx, dword ptr [ebp-0xf4]
0x08048b25   mov ecx, dword ptr [ecx+0x30]
0x08048b28   mov ecx, dword ptr [ebp+ecx*4-0xf0]
0x08048b2f   mov dword ptr [ecx], eax
0x08048b31   mov eax, dword ptr [ebp-0xf4]
0x08048b37   add eax, 0x34
0x08048b3a   mov dword ptr [ebp-0xf4], eax
0x08048b40   jmp 0x8049762
```

```
11
0x08048e4c   mov eax, dword ptr [ebp-0xf4]
0x08048e52   add eax, 0x1
0x08048e55   mov dword ptr [ebp-0xf4], eax
0x08048e5b   mov eax, dword ptr [ebp-0xf4]
0x08048e61   mov eax, dword ptr [eax+0x4]
0x08048e64   mov ecx, dword ptr [ebp-0xf4]
0x08048e6a   mov ecx, dword ptr [ecx]
0x08048e6c   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048e73   mov eax, dword ptr [ebp-0xf4]
0x08048e79   add eax, 0x8
0x08048e7c   mov dword ptr [ebp-0xf4], eax
0x08048e82   jmp 0x8049762
```

```
12
0x080485f5   jmp 0x80485fa
0x080485fa   mov eax, dword ptr [ebp-0xf8]
0x08048600   sub eax, 0x24
0x08048603   mov dword ptr [ebp-0x11c], eax
0x08048609   jz 0x804967c
```

```
13
0x0804862e   mov eax, dword ptr [ebp-0xf8]
0x08048634   sub eax, 0x3a
0x08048637   mov dword ptr [ebp-0x124], eax
0x0804863d   jnle 0x804867c
```

```
14
0x080486c7   jmp 0x80486cc
0x080486cc   mov eax, dword ptr [ebp-0xf8]
0x080486d2   sub eax, 0x71
0x080486d5   mov dword ptr [ebp-0x13c], eax
0x080486db   jnle 0x804871a
```

```
15
0x0804874e   mov eax, dword ptr [ebp-0xf8]
0x08048754   sub eax, 0xa6
0x08048759   mov dword ptr [ebp-0x150], eax
0x0804875f   jnle 0x804879b
```

```
16
0x08048c19   jmp 0x8048c1e
0x08048c1e   mov eax, dword ptr [ebp-0x188]
0x08048c24   sub eax, 0x1
0x08048c27   mov dword ptr [ebp-0x18c], eax
0x08048c2d   jnz 0x8048c61
0x08048c33   jmp 0x8048c38
0x08048c38   lea eax, ptr [ebp-0x10]
0x08048c3b   mov ecx, dword ptr [ebp-0xf4]
0x08048c41   mov ecx, dword ptr [ecx]
0x08048c43   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048c4a   jmp 0x8048c61
```

```
17
0x08048c4f   lea eax, ptr [ebp-0xc]
0x08048c52   mov ecx, dword ptr [ebp-0xf4]
0x08048c58   mov ecx, dword ptr [ecx]
0x08048c5a   mov dword ptr [ebp+ecx*4-0xf0], eax
```

```
20
0x08049762   jmp 0x804851f
```

```
21
0x0804860f   jmp 0x8048614
0x08048614   mov eax, dword ptr [ebp-0xf8]
0x0804861a   sub eax, 0x26
0x0804861d   mov dword ptr [ebp-0x120], eax
0x08048623   jz 0x80488f7
0x080488f7   lea eax, ptr [ebp-0x34]
0x080488fa   mov ecx, dword ptr [ebp-0xf4]
0x08048900   add ecx, 0x1
0x08048903   mov dword ptr [ebp-0xf4], ecx
0x08048909   mov ecx, dword ptr [ebp-0xf4]
0x0804890f   add eax, dword ptr [ecx]
0x08048911   mov ecx, dword ptr [ebp-0xf4]
0x08048917   mov ecx, dword ptr [ecx+0x4]
0x0804891a   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048921   mov eax, dword ptr [ebp-0xf4]
0x08048927   mov eax, dword ptr [eax+0x8]
0x0804892a   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048931   mov eax, dword ptr [eax]
0x08048933   mov ecx, dword ptr [ebp-0xf4]
0x08048939   mov ecx, dword ptr [ecx+0xc]
0x0804893c   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048943   mov eax, dword ptr [ebp-0xf4]
0x08048949   mov eax, dword ptr [eax+0x10]
0x0804894c   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048953   mov ecx, dword ptr [ebp-0xbc]
0x08048959   mov dword ptr [ecx+0x4], eax
0x0804895c   mov eax, dword ptr [ebp-0xf4]
0x08048962   mov eax, dword ptr [eax+0x14]
0x08048965   mov ecx, dword ptr [ebp-0xf4]
0x0804896b   mov ecx, dword ptr [ecx+0x18]
0x0804896e   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048975   mov eax, dword ptr [ebp-0xbc]
0x0804897b   add eax, 0x4
0x0804897e   mov dword ptr [ebp-0xbc], eax
0x08048984   mov eax, dword ptr [ebp-0xf4]
0x0804898a   add eax, 0x1c
0x0804898d   mov dword ptr [ebp-0xf4], eax
0x08048993   jmp 0x8049762
```

```
22
0x0804967c   mov eax, dword ptr [ebp-0xf4]
0x08049682   add eax, 0x1
0x08049685   mov dword ptr [ebp-0xf4], eax
0x0804968b   mov eax, dword ptr [ebp-0xbc]
0x08049691   mov eax, dword ptr [eax]
0x08049693   mov ecx, dword ptr [ebp-0xbc]
0x08049699   imul eax, dword ptr [ecx-0x4]
0x0804969d   mov ecx, dword ptr [ebp-0xf4]
0x080496a3   mov ecx, dword ptr [ecx]
0x080496a5   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080496ac   mov eax, dword ptr [ebp-0xf4]
0x080496b2   mov eax, dword ptr [eax+0x4]
0x080496b5   mov eax, dword ptr [ebp+eax*4-0xf0]
0x080496bc   mov ecx, dword ptr [ebp-0xbc]
0x080496c2   mov dword ptr [ecx-0x4], eax
0x080496c5   mov eax, dword ptr [ebp-0xbc]
0x080496cb   add eax, 0xfffffffc
0x080496ce   mov dword ptr [ebp-0xbc], eax
0x080496d4   mov eax, dword ptr [ebp-0xf4]
0x080496da   add eax, 0x8
0x080496dd   mov dword ptr [ebp-0xf4], eax
0x080496e3   jmp 0x8049762
```

```
23
0x08048643   jmp 0x8048648
0x08048648   mov eax, dword ptr [ebp-0xf8]
0x0804864e   sub eax, 0x34
0x08048651   mov dword ptr [ebp-0x128], eax
0x08048657   jz 0x8048e87
0x08048e87   mov eax, dword ptr [ebp-0xf4]
0x08048e8d   add eax, 0x1
0x08048e90   mov dword ptr [ebp-0xf4], eax
0x08048e96   mov eax, dword ptr [ebp-0xf4]
0x08048e9c   mov eax, dword ptr [eax]
0x08048e9e   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048ea5   mov eax, dword ptr [eax]
0x08048ea7   mov ecx, dword ptr [ebp-0xf4]
0x08048ead   mov ecx, dword ptr [ecx+0x8]
0x08048eb0   cmp eax, dword ptr [ebp+ecx*4-0xf0]
0x08048eb7   setnle dl
0x08048eba   and dl, 0x1
0x08048ebd   movzx eax, dl
0x08048ec0   mov ecx, dword ptr [ebp-0xf4]
0x08048ec6   mov ecx, dword ptr [ecx+0x4]
0x08048ec9   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048ed0   mov eax, dword ptr [ebp-0xf4]
0x08048ed6   mov eax, dword ptr [eax+0xc]
0x08048ed9   cmp dword ptr [ebp+eax*4-0xf0], 0x0
0x08048ee1   jz 0x8048f01
```

```
24
0x0804867c   mov eax, dword ptr [ebp-0xf8]
0x08048682   sub eax, 0x3b
0x08048685   mov dword ptr [ebp-0x130], eax
0x0804868b   jz 0x80491cf
```

```
25
0x080486e1   jmp 0x80486e6
0x080486e6   mov eax, dword ptr [ebp-0xf8]
0x080486ec   sub eax, 0x5a
0x080486ef   mov dword ptr [ebp-0x140], eax
0x080486f5   jz 0x8048998
```

```
26
0x0804871a   mov eax, dword ptr [ebp-0xf8]
0x08048720   sub eax, 0x72
0x08048723   mov dword ptr [ebp-0x148], eax
0x08048729   jz 0x8049010
```

```
27
0x08048765   jmp 0x804876a
0x0804876a   mov eax, dword ptr [ebp-0xf8]
0x08048770   add eax, 0xffffff6b
0x08048775   mov ecx, eax
0x08048777   sub ecx, 0x8
0x0804877a   mov dword ptr [ebp-0x154], eax
0x08048780   mov dword ptr [ebp-0x158], ecx
0x08048786   jnbe 0x8049762
0x0804878c   mov eax, dword ptr [ebp-0x154]
0x08048792   mov ecx, dword ptr [eax*4+0x8049904]
0x08048799   jmp ecx
```

```
28
0x0804879b   mov eax, dword ptr [ebp-0xf8]
0x080487a1   sub eax, 0xfc
0x080487a6   mov dword ptr [ebp-0x15c], eax
0x080487ac   jnle 0x80488b3
```

```
30
0x08048c61   mov eax, dword ptr [ebp-0xf4]
0x08048c67   add eax, 0x8
0x08048c6a   mov dword ptr [ebp-0xf4], eax
0x08048c70   jmp 0x8049762
```

```
31
0x08048ee7   mov eax, dword ptr [ebp-0xf4]
0x08048eed   mov eax, dword ptr [eax+0x10]
0x08048ef0   add eax, dword ptr [ebp-0xf4]
0x08048ef6   mov dword ptr [ebp-0xf4], eax
0x08048efc   jmp 0x8048f10
```

```
32
0x08048f01   mov eax, dword ptr [ebp-0xf4]
0x08048f07   add eax, 0x14
0x08048f0a   mov dword ptr [ebp-0xf4], eax
```

```
33
0x08048691   jmp 0x8048696
0x08048696   mov eax, dword ptr [ebp-0xf8]
0x0804869c   sub eax, 0x44
0x0804869f   mov dword ptr [ebp-0x134], eax
0x080486a5   jz 0x804944b
0x0804944b   mov eax, dword ptr [ebp-0xf4]
0x08049451   add eax, 0x1
0x08049454   mov dword ptr [ebp-0xf4], eax
0x0804945a   mov eax, dword ptr [ebp-0xf4]
0x08049460   mov eax, dword ptr [eax]
0x08049462   mov eax, dword ptr [ebp+eax*1-0x34]
0x08049466   mov ecx, dword ptr [ebp-0xf4]
0x0804946c   mov ecx, dword ptr [ecx+0x4]
0x0804946f   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049476   mov eax, dword ptr [ebp-0xf4]
0x0804947c   mov eax, dword ptr [eax+0xc]
0x0804947f   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049486   mov ecx, dword ptr [ebp-0xf4]
0x0804948c   mov ecx, dword ptr [ecx+0x8]
0x0804948f   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049496   mov eax, dword ptr [ebp-0xf4]
0x0804949c   mov eax, dword ptr [eax+0x10]
0x0804949f   mov ecx, dword ptr [ebp-0xf4]
0x080494a5   mov ecx, dword ptr [ecx+0x18]
0x080494a8   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080494af   mov eax, dword ptr [ebp-0xf4]
0x080494b5   mov eax, dword ptr [eax+0x20]
0x080494b8   mov eax, dword ptr [ebp+eax*4-0xf0]
0x080494bf   mov ecx, dword ptr [ebp-0xf4]
0x080494c5   mov ecx, dword ptr [ecx+0x1c]
0x080494c8   imul eax, dword ptr [ebp+ecx*4-0xf0]
0x080494d0   mov ecx, dword ptr [ebp-0xf4]
0x080494d6   mov ecx, dword ptr [ecx+0x24]
0x080494d9   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080494e0   mov eax, dword ptr [ebp-0xbc]
0x080494e6   mov eax, dword ptr [eax]
0x080494e8   mov eax, dword ptr [eax]
0x080494ea   mov ecx, dword ptr [ebp-0xf4]
0x080494f0   mov ecx, dword ptr [ecx+0x28]
0x080494f3   add eax, dword ptr [ebp+ecx*4-0xf0]
0x080494fa   mov ecx, dword ptr [ebp-0xbc]
0x08049500   mov dword ptr [ecx], eax
0x08049502   mov eax, dword ptr [ebp-0xf4]
0x08049508   add eax, 0x2c
0x0804950b   mov dword ptr [ebp-0xf4], eax
0x08049511   jmp 0x8049762
```

```
34
0x080491cf   mov eax, dword ptr [ebp-0xf4]
0x080491d5   add eax, 0x1
0x080491d8   mov dword ptr [ebp-0xf4], eax
0x080491de   mov eax, dword ptr [ebp-0xbc]
0x080491e4   mov eax, dword ptr [eax]
0x080491e6   mov ecx, dword ptr [ebp-0xf4]
0x080491ec   mov ecx, dword ptr [ecx]
0x080491ee   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080491f5   mov eax, dword ptr [ebp-0xf4]
0x080491fb   mov eax, dword ptr [eax+0x4]
0x080491fe   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049205   mov eax, dword ptr [eax]
0x08049207   mov ecx, dword ptr [ebp-0xbc]
0x0804920d   mov dword ptr [ecx], eax
0x0804920f   mov eax, dword ptr [ebp-0xf4]
0x08049215   mov eax, dword ptr [eax+0x8]
0x08049218   mov ecx, dword ptr [ebp-0xf4]
0x0804921e   mov ecx, dword ptr [ecx+0x10]
0x08049221   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049228   mov eax, dword ptr [ebp-0xf4]
0x0804922e   mov eax, dword ptr [eax+0x18]
0x08049231   mov eax, dword ptr [ebp+eax*1-0x34]
0x08049235   mov ecx, dword ptr [ebp-0xf4]
0x0804923b   mov ecx, dword ptr [ecx+0x1c]
0x0804923e   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049245   mov eax, dword ptr [ebp-0xf4]
0x0804924b   mov eax, dword ptr [eax+0x24]
0x0804924e   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049255   mov ecx, dword ptr [ebp-0xf4]
0x0804925b   mov ecx, dword ptr [ecx+0x20]
0x0804925e   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049265   mov eax, dword ptr [ebp-0xf4]
0x0804926b   mov eax, dword ptr [eax+0x28]
0x0804926e   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049275   mov ecx, dword ptr [ebp-0xf4]
0x0804927b   mov ecx, dword ptr [ecx+0x14]
0x0804927e   imul eax, dword ptr [ebp+ecx*4-0xf0]
0x08049286   mov ecx, dword ptr [ebp-0xf4]
0x0804928c   mov ecx, dword ptr [ecx+0x2c]
0x0804928f   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049296   mov eax, dword ptr [ebp-0xf4]
0x0804929c   add eax, 0x30
0x0804929f   mov dword ptr [ebp-0xf4], eax
0x080492a5   jmp 0x8049762
```

```
35
0x080486fb   jmp 0x8048700
0x08048700   mov eax, dword ptr [ebp-0xf8]
0x08048706   sub eax, 0x5f
0x08048709   mov dword ptr [ebp-0x144], eax
0x0804870f   jz 0x804934b
0x0804934b   mov eax, dword ptr [ebp-0xf4]
0x08049351   add eax, 0x1
0x08049354   mov dword ptr [ebp-0xf4], eax
0x0804935a   mov eax, dword ptr [ebp-0xf4]
0x08049360   mov eax, dword ptr [eax+0x8]
0x08049363   mov ecx, dword ptr [ebp-0xf4]
0x08049369   mov ecx, dword ptr [ecx+0x4]
0x0804936c   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049373   mov eax, dword ptr [ebp-0xf4]
0x08049379   mov eax, dword ptr [eax+0xc]
0x0804937c   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049383   mov ecx, dword ptr [ebp-0xf4]
0x08049389   mov ecx, dword ptr [ecx]
0x0804938b   mov dword ptr [ebp+ecx*1-0x34], eax
0x0804938f   mov eax, dword ptr [ebp-0xf4]
0x08049395   mov eax, dword ptr [eax+0x10]
0x08049398   add eax, dword ptr [ebp-0xf4]
0x0804939e   mov dword ptr [ebp-0xf4], eax
0x080493a4   jmp 0x8049762
```

```
36
0x08048998   mov eax, dword ptr [ebp-0xf4]
0x0804899e   add eax, 0x1
0x080489a1   mov dword ptr [ebp-0xf4], eax
0x080489a7   mov eax, dword ptr [ebp-0xf4]
0x080489ad   mov eax, dword ptr [eax]
0x080489af   mov eax, dword ptr [ebp+eax*4-0xf0]
0x080489b6   mov eax, dword ptr [eax]
0x080489b8   mov ecx, dword ptr [ebp-0xf4]
0x080489be   mov ecx, dword ptr [ecx+0x4]
0x080489c1   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080489c8   mov eax, dword ptr [ebp-0xbc]
0x080489ce   mov eax, dword ptr [eax]
0x080489d0   mov ecx, dword ptr [ebp-0xf4]
0x080489d6   mov ecx, dword ptr [ecx+0x8]
0x080489d9   mov ecx, dword ptr [ebp+ecx*4-0xf0]
0x080489e0   mov edx, dword ptr [ebp-0xf4]
0x080489e6   mov edx, dword ptr [edx+0xc]
0x080489e9   sub ecx, dword ptr [ebp+edx*4-0xf0]
0x080489f0   cmp eax, ecx
0x080489f2   setl bl
0x080489f5   and bl, 0x1
0x080489f8   movzx eax, bl
0x080489fb   mov ecx, dword ptr [ebp-0xf4]
0x08048a01   mov ecx, dword ptr [ecx+0x10]
0x08048a04   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048a0b   mov eax, dword ptr [ebp-0xf4]
0x08048a11   mov eax, dword ptr [eax+0x14]
0x08048a14   cmp dword ptr [ebp+eax*4-0xf0], 0x0
0x08048a1c   jz 0x8048a3c
```

```
37
0x0804872f   jmp 0x8048734
0x08048734   mov eax, dword ptr [ebp-0xf8]
0x0804873a   sub eax, 0x7f
0x0804873d   mov dword ptr [ebp-0x14c], eax
0x08048743   jz 0x80492aa
0x080492aa   mov eax, dword ptr [ebp-0xf4]
0x080492b0   add eax, 0x1
0x080492b3   mov dword ptr [ebp-0xf4], eax
0x080492b9   mov eax, dword ptr [ebp-0xbc]
0x080492bf   mov eax, dword ptr [eax]
0x080492c1   mov eax, dword ptr [eax]
0x080492c3   mov ecx, dword ptr [ebp-0xbc]
0x080492c9   mov ecx, dword ptr [ecx-0x4]
0x080492cc   mov eax, dword ptr [eax+ecx*1]
0x080492cf   mov ecx, dword ptr [ebp-0xf4]
0x080492d5   mov ecx, dword ptr [ecx+0x4]
0x080492d8   cmp eax, dword ptr [ebp+ecx*4-0xf0]
0x080492df   setnle dl
0x080492e2   and dl, 0x1
0x080492e5   movzx eax, dl
0x080492e8   mov ecx, dword ptr [ebp-0xf4]
0x080492ee   mov ecx, dword ptr [ecx]
0x080492f0   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080492f7   mov eax, dword ptr [ebp-0xf4]
0x080492fd   mov eax, dword ptr [eax+0x8]
0x08049300   cmp dword ptr [ebp+eax*4-0xf0], 0x0
0x08049308   jz 0x8049328
```

```
38
0x08049010   mov eax, dword ptr [ebp-0xf4]
0x08049016   add eax, 0x1
0x08049019   mov dword ptr [ebp-0xf4], eax
0x0804901f   mov eax, dword ptr [ebp-0xbc]
0x08049025   mov eax, dword ptr [eax]
0x08049027   mov eax, dword ptr [eax]
0x08049029   mov ecx, dword ptr [ebp-0xbc]
0x0804902f   add eax, dword ptr [ecx-0x4]
0x08049032   mov ecx, dword ptr [ebp-0xbc]
0x08049038   mov dword ptr [ecx-0x4], eax
0x0804903b   mov eax, dword ptr [ebp-0xf4]
0x08049041   mov eax, dword ptr [eax]
0x08049043   mov eax, dword ptr [ebp+eax*1-0x34]
0x08049047   mov ecx, dword ptr [ebp-0xf4]
0x0804904d   mov ecx, dword ptr [ecx+0x4]
0x08049050   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049057   mov eax, dword ptr [ebp-0xf4]
0x0804905d   mov eax, dword ptr [eax+0x8]
0x08049060   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049067   mov ecx, dword ptr [ebp-0xbc]
0x0804906d   mov ecx, dword ptr [ecx-0x4]
0x08049070   mov dword ptr [ecx], eax
0x08049072   mov eax, dword ptr [ebp-0xf4]
0x08049078   mov eax, dword ptr [eax+0xc]
0x0804907b   add eax, dword ptr [ebp-0xf4]
0x08049081   mov dword ptr [ebp-0xf4], eax
0x08049087   mov eax, dword ptr [ebp-0xbc]
0x0804908d   add eax, 0xfffffff8
0x08049090   mov dword ptr [ebp-0xbc], eax
0x08049096   jmp 0x8049762
```

```
39
0x080488cf   mov eax, dword ptr [ebp-0xf4]
0x080488d5   add eax, 0x1
0x080488d8   mov dword ptr [ebp-0xf4], eax
0x080488de   mov eax, dword ptr [ebp-0xf4]
0x080488e4   mov eax, dword ptr [eax]
0x080488e6   add eax, dword ptr [ebp-0xf4]
0x080488ec   mov dword ptr [ebp-0xf4], eax
0x080488f2   jmp 0x8049762
```

```
40
0x08048d0f   mov eax, dword ptr [ebp-0xf4]
0x08048d15   add eax, 0x1
0x08048d18   mov dword ptr [ebp-0xf4], eax
0x08048d1e   mov eax, dword ptr [ebp-0xf4]
0x08048d24   mov eax, dword ptr [eax]
0x08048d26   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048d2d   mov eax, dword ptr [eax]
0x08048d2f   mov ecx, dword ptr [ebp-0xbc]
0x08048d35   mov ecx, dword ptr [ecx]
0x08048d37   mov eax, dword ptr [eax+ecx*1]
0x08048d3a   mov ecx, dword ptr [ebp-0xf4]
0x08048d40   mov ecx, dword ptr [ecx+0x4]
0x08048d43   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048d4a   mov eax, dword ptr [ebp-0xf4]
0x08048d50   mov eax, dword ptr [eax+0x8]
0x08048d53   mov ecx, dword ptr [ebp-0xbc]
0x08048d59   mov dword ptr [ecx], eax
0x08048d5b   mov eax, dword ptr [ebp-0xf4]
0x08048d61   mov eax, dword ptr [eax+0x10]
0x08048d64   mov eax, dword ptr [ebp+eax*1-0x34]
0x08048d68   mov ecx, dword ptr [ebp-0xf4]
0x08048d6e   mov ecx, dword ptr [ecx+0x14]
0x08048d71   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048d78   mov eax, dword ptr [ebp-0xf4]
0x08048d7e   mov eax, dword ptr [eax+0x1c]
0x08048d81   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048d88   mov ecx, dword ptr [ebp-0xf4]
0x08048d8e   mov ecx, dword ptr [ecx+0x18]
0x08048d91   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048d98   mov eax, dword ptr [ebp-0xf4]
0x08048d9e   mov eax, dword ptr [eax+0x20]
0x08048da1   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048da8   mov ecx, dword ptr [ebp-0xbc]
0x08048dae   mov dword ptr [ecx+0x4], eax
0x08048db1   mov eax, dword ptr [ebp-0xbc]
0x08048db7   add eax, 0x4
0x08048dba   mov dword ptr [ebp-0xbc], eax
0x08048dc0   mov eax, dword ptr [ebp-0xf4]
0x08048dc6   add eax, 0x24
0x08048dc9   mov dword ptr [ebp-0xf4], eax
0x08048dcf   jmp 0x8049762
```

```
41
0x08049516   mov eax, dword ptr [ebp-0xf4]
0x0804951c   add eax, 0x1
0x0804951f   mov dword ptr [ebp-0xf4], eax
0x08049525   mov eax, dword ptr [ebp-0xf4]
0x0804952b   mov eax, dword ptr [eax+0x4]
0x0804952e   mov ecx, dword ptr [ebp-0xf4]
0x08049534   mov ecx, dword ptr [ecx]
0x08049536   mov dword ptr [ebp+ecx*4-0xf0], eax
0x0804953d   mov eax, dword ptr [ebp-0xf4]
0x08049543   mov eax, dword ptr [eax+0x8]
0x08049546   mov eax, dword ptr [ebp+eax*1-0x34]
0x0804954a   mov ecx, dword ptr [ebp-0xf4]
0x08049550   mov ecx, dword ptr [ecx+0xc]
0x08049553   mov dword ptr [ebp+ecx*4-0xf0], eax
0x0804955a   mov eax, dword ptr [ebp-0xf4]
0x08049560   mov eax, dword ptr [eax+0x10]
0x08049563   mov eax, dword ptr [ebp+eax*4-0xf0]
0x0804956a   mov ecx, dword ptr [ebp-0xf4]
0x08049570   mov ecx, dword ptr [ecx+0x14]
0x08049573   add eax, dword ptr [ebp+ecx*4-0xf0]
0x0804957a   mov ecx, dword ptr [ebp-0xf4]
0x08049580   mov ecx, dword ptr [ecx+0x18]
0x08049583   mov dword ptr [ebp+ecx*4-0xf0], eax
0x0804958a   mov eax, dword ptr [ebp-0xf4]
0x08049590   mov eax, dword ptr [eax+0x20]
0x08049593   mov eax, dword ptr [ebp+eax*4-0xf0]
0x0804959a   mov ecx, dword ptr [ebp-0xf4]
0x080495a0   mov ecx, dword ptr [ecx+0x1c]
0x080495a3   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080495aa   mov eax, dword ptr [ebp-0xf4]
0x080495b0   mov eax, dword ptr [eax+0x24]
0x080495b3   mov ecx, dword ptr [ebp-0xf4]
0x080495b9   mov ecx, dword ptr [ecx+0x2c]
0x080495bc   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080495c3   mov eax, dword ptr [ebp-0xf4]
0x080495c9   mov eax, dword ptr [eax+0x34]
0x080495cc   mov eax, dword ptr [ebp+eax*4-0xf0]
0x080495d3   mov ecx, dword ptr [ebp-0xf4]
0x080495d9   mov ecx, dword ptr [ecx+0x30]
0x080495dc   imul eax, dword ptr [ebp+ecx*4-0xf0]
0x080495e4   mov ecx, dword ptr [ebp-0xf4]
0x080495ea   mov ecx, dword ptr [ecx+0x38]
0x080495ed   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080495f4   mov eax, dword ptr [ebp-0xf4]
0x080495fa   mov eax, dword ptr [eax+0x3c]
0x080495fd   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08049604   mov ecx, dword ptr [ebp-0xbc]
0x0804960a   mov dword ptr [ecx+0x4], eax
0x0804960d   mov eax, dword ptr [ebp-0xbc]
0x08049613   add eax, 0x4
0x08049616   mov dword ptr [ebp-0xbc], eax
0x0804961c   mov eax, dword ptr [ebp-0xf4]
0x08049622   add eax, 0x40
0x08049625   mov dword ptr [ebp-0xf4], eax
0x0804962b   jmp 0x8049762
```

```
42
0x08049630   mov eax, dword ptr [ebp-0xf4]
0x08049636   mov ecx, eax
0x08049638   inc ecx
0x08049639   mov dword ptr [ebp-0xf4], ecx
0x0804963f   mov eax, dword ptr [eax+0x1]
0x08049642   sub eax, 0x1
0x08049645   mov dword ptr [ebp-0x190], eax
0x0804964b   jnz 0x8049668
0x08049651   jmp 0x8049656
0x08049656   mov eax, dword ptr [ebp-0x1c]
0x08049659   mov ecx, dword ptr [ebp-0x14]
0x0804965c   mov dword ptr [esp], eax
0x0804965f   mov dword ptr [esp+0x4], ecx
0x08049663   call 0x80484f0
```

```
43
0x080487b2   jmp 0x80487b7
0x080487b7   mov eax, dword ptr [ebp-0xf8]
0x080487bd   sub eax, 0xb6
0x080487c2   mov dword ptr [ebp-0x160], eax
0x080487c8   jnle 0x80487ef
```

```
44
0x080488b3   mov eax, dword ptr [ebp-0xf8]
0x080488b9   sub eax, 0xfd
0x080488be   mov dword ptr [ebp-0x184], eax
0x080488c4   jz 0x80496e8
0x080496e8   mov eax, dword ptr [ebp-0xf4]
0x080496ee   mov ecx, eax
0x080496f0   inc ecx
0x080496f1   mov dword ptr [ebp-0xf4], ecx
0x080496f7   mov eax, dword ptr [eax+0x1]
0x080496fa   test eax, eax
0x080496fc   mov dword ptr [ebp-0x194], eax
0x08049702   jz 0x8049738
```

```
46
0x08048f10   jmp 0x8049762
```

```
47
0x08048a22   mov eax, dword ptr [ebp-0xf4]
0x08048a28   mov eax, dword ptr [eax+0x18]
0x08048a2b   add eax, dword ptr [ebp-0xf4]
0x08048a31   mov dword ptr [ebp-0xf4], eax
0x08048a37   jmp 0x8048a4b
```

```
48
0x08048a3c   mov eax, dword ptr [ebp-0xf4]
0x08048a42   add eax, 0x1c
0x08048a45   mov dword ptr [ebp-0xf4], eax
```

```
49
0x0804930e   mov eax, dword ptr [ebp-0xf4]
0x08049314   mov eax, dword ptr [eax+0xc]
0x08049317   add eax, dword ptr [ebp-0xf4]
0x0804931d   mov dword ptr [ebp-0xf4], eax
0x08049323   jmp 0x8049337
```

```
50
0x08049328   mov eax, dword ptr [ebp-0xf4]
0x0804932e   add eax, 0x10
0x08049331   mov dword ptr [ebp-0xf4], eax
```

```
51
0x080487ce   jmp 0x80487d3
0x080487d3   mov eax, dword ptr [ebp-0xf8]
0x080487d9   sub eax, 0xa7
0x080487de   mov dword ptr [ebp-0x164], eax
0x080487e4   jz 0x8048f15
0x08048f15   mov eax, dword ptr [ebp-0xf4]
0x08048f1b   add eax, 0x1
0x08048f1e   mov dword ptr [ebp-0xf4], eax
0x08048f24   mov eax, dword ptr [ebp-0xbc]
0x08048f2a   mov eax, dword ptr [eax]
0x08048f2c   mov ecx, dword ptr [ebp-0xf4]
0x08048f32   mov ecx, dword ptr [ecx]
0x08048f34   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048f3b   mov eax, dword ptr [ebp-0xf4]
0x08048f41   mov eax, dword ptr [eax+0x4]
0x08048f44   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048f4b   mov eax, dword ptr [eax]
0x08048f4d   mov ecx, dword ptr [ebp-0xbc]
0x08048f53   mov dword ptr [ecx], eax
0x08048f55   mov eax, dword ptr [ebp-0xf4]
0x08048f5b   mov eax, dword ptr [eax+0x8]
0x08048f5e   mov eax, dword ptr [ebp+eax*1-0x34]
0x08048f62   mov ecx, dword ptr [ebp-0xf4]
0x08048f68   mov ecx, dword ptr [ecx+0xc]
0x08048f6b   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048f72   mov eax, dword ptr [ebp-0xf4]
0x08048f78   mov eax, dword ptr [eax+0x18]
0x08048f7b   mov ecx, dword ptr [ebp-0xf4]
0x08048f81   mov ecx, dword ptr [ecx+0x14]
0x08048f84   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048f8b   mov eax, dword ptr [ebp-0xf4]
0x08048f91   mov eax, dword ptr [eax+0x10]
0x08048f94   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048f9b   mov ecx, dword ptr [ebp-0xf4]
0x08048fa1   mov ecx, dword ptr [ecx+0x1c]
0x08048fa4   add eax, dword ptr [ebp+ecx*4-0xf0]
0x08048fab   mov ecx, dword ptr [ebp-0xf4]
0x08048fb1   mov ecx, dword ptr [ecx+0x20]
0x08048fb4   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048fbb   mov eax, dword ptr [ebp-0xf4]
0x08048fc1   mov eax, dword ptr [eax+0x28]
0x08048fc4   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048fcb   mov ecx, dword ptr [ebp-0xf4]
0x08048fd1   mov ecx, dword ptr [ecx+0x24]
0x08048fd4   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048fdb   mov eax, dword ptr [ebp-0xf4]
0x08048fe1   mov eax, dword ptr [eax+0x2c]
0x08048fe4   mov ecx, dword ptr [ebp-0xbc]
0x08048fea   mov dword ptr [ecx+0x4], eax
0x08048fed   mov eax, dword ptr [ebp-0xbc]
0x08048ff3   add eax, 0x4
0x08048ff6   mov dword ptr [ebp-0xbc], eax
0x08048ffc   mov eax, dword ptr [ebp-0xf4]
0x08049002   add eax, 0x34
0x08049005   mov dword ptr [ebp-0xf4], eax
0x0804900b   jmp 0x8049762
```

```
52
0x080487ef   mov eax, dword ptr [ebp-0xf8]
0x080487f5   sub eax, 0xc2
0x080487fa   mov dword ptr [ebp-0x168], eax
0x08048800   jnle 0x8048827
```

```
53
0x08049708   jmp 0x804970d
0x0804970d   mov eax, dword ptr [ebp-0x194]
0x08049713   sub eax, 0x1
0x08049716   mov dword ptr [ebp-0x198], eax
0x0804971c   jnz 0x8049744
0x08049722   jmp 0x8049727
0x08049727   lea eax, ptr [ebp-0x10]
0x0804972a   mov ecx, dword ptr [ebp-0xbc]
0x08049730   mov dword ptr [ecx+0x4], eax
0x08049733   jmp 0x8049744
```

```
54
0x08049738   lea eax, ptr [ebp-0xc]
0x0804973b   mov ecx, dword ptr [ebp-0xbc]
0x08049741   mov dword ptr [ecx+0x4], eax
```

```
56
0x08048a4b   mov eax, dword ptr [ebp-0xbc]
0x08048a51   add eax, 0xfffffffc
0x08048a54   mov dword ptr [ebp-0xbc], eax
0x08048a5a   jmp 0x8049762
```

```
58
0x08049337   mov eax, dword ptr [ebp-0xbc]
0x0804933d   add eax, 0xfffffff8
0x08049340   mov dword ptr [ebp-0xbc], eax
0x08049346   jmp 0x8049762
```

```
59
0x08048806   jmp 0x804880b
0x0804880b   mov eax, dword ptr [ebp-0xf8]
0x08048811   sub eax, 0xb7
0x08048816   mov dword ptr [ebp-0x16c], eax
0x0804881c   jz 0x8048b45
0x08048b45   mov eax, dword ptr [ebp-0xf4]
0x08048b4b   add eax, 0x1
0x08048b4e   mov dword ptr [ebp-0xf4], eax
0x08048b54   mov eax, dword ptr [ebp-0xf4]
0x08048b5a   mov eax, dword ptr [eax+0x4]
0x08048b5d   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048b64   mov ecx, dword ptr [ebp-0xf4]
0x08048b6a   mov ecx, dword ptr [ecx]
0x08048b6c   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048b73   mov eax, dword ptr [ebp-0xf4]
0x08048b79   mov eax, dword ptr [eax+0x8]
0x08048b7c   mov ecx, dword ptr [ebp-0xf4]
0x08048b82   mov ecx, dword ptr [ecx+0x10]
0x08048b85   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048b8c   mov eax, dword ptr [ebp-0xf4]
0x08048b92   mov eax, dword ptr [eax+0x18]
0x08048b95   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048b9c   mov ecx, dword ptr [ebp-0xf4]
0x08048ba2   mov ecx, dword ptr [ecx+0x14]
0x08048ba5   imul eax, dword ptr [ebp+ecx*4-0xf0]
0x08048bad   mov ecx, dword ptr [ebp-0xf4]
0x08048bb3   mov ecx, dword ptr [ecx+0x1c]
0x08048bb6   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048bbd   mov eax, dword ptr [ebp-0xf4]
0x08048bc3   mov eax, dword ptr [eax+0x20]
0x08048bc6   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048bcd   mov ecx, dword ptr [ebp-0xbc]
0x08048bd3   mov dword ptr [ecx+0x4], eax
0x08048bd6   mov eax, dword ptr [ebp-0xbc]
0x08048bdc   add eax, 0x4
0x08048bdf   mov dword ptr [ebp-0xbc], eax
0x08048be5   mov eax, dword ptr [ebp-0xf4]
0x08048beb   add eax, 0x24
0x08048bee   mov dword ptr [ebp-0xf4], eax
0x08048bf4   jmp 0x8049762
```

```
60
0x08048827   mov eax, dword ptr [ebp-0xf8]
0x0804882d   sub eax, 0xcb
0x08048832   mov dword ptr [ebp-0x170], eax
0x08048838   jnle 0x804887b
```

```
62
0x08049744   mov eax, dword ptr [ebp-0xbc]
0x0804974a   add eax, 0x4
0x0804974d   mov dword ptr [ebp-0xbc], eax
0x08049753   mov eax, dword ptr [ebp-0xf4]
0x08049759   add eax, 0x4
0x0804975c   mov dword ptr [ebp-0xf4], eax
```

```
63
0x0804883e   jmp 0x8048843
0x08048843   mov eax, dword ptr [ebp-0xf8]
0x08048849   sub eax, 0xc3
0x0804884e   mov dword ptr [ebp-0x174], eax
0x08048854   jz 0x804909b
```

```
64
0x0804887b   mov eax, dword ptr [ebp-0xf8]
0x08048881   sub eax, 0xcc
0x08048886   mov dword ptr [ebp-0x17c], eax
0x0804888c   jz 0x80493a9
```

```
65
0x0804885a   jmp 0x804885f
0x0804885f   mov eax, dword ptr [ebp-0xf8]
0x08048865   sub eax, 0xc4
0x0804886a   mov dword ptr [ebp-0x178], eax
0x08048870   jz 0x8048dd4
0x08048dd4   mov eax, dword ptr [ebp-0xf4]
0x08048dda   add eax, 0x1
0x08048ddd   mov dword ptr [ebp-0xf4], eax
0x08048de3   mov eax, dword ptr [ebp-0xbc]
0x08048de9   mov eax, dword ptr [eax]
0x08048deb   mov eax, dword ptr [eax]
0x08048ded   mov ecx, dword ptr [ebp-0xf4]
0x08048df3   mov ecx, dword ptr [ecx]
0x08048df5   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048dfc   mov eax, dword ptr [ebp-0xf4]
0x08048e02   mov eax, dword ptr [eax+0x4]
0x08048e05   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048e0c   mov ecx, dword ptr [ebp-0xf4]
0x08048e12   mov ecx, dword ptr [ecx+0x8]
0x08048e15   sub eax, dword ptr [ebp+ecx*4-0xf0]
0x08048e1c   mov ecx, dword ptr [ebp-0xf4]
0x08048e22   mov ecx, dword ptr [ecx+0xc]
0x08048e25   mov dword ptr [ebp+ecx*1-0x34], eax
0x08048e29   mov eax, dword ptr [ebp-0xbc]
0x08048e2f   add eax, 0xfffffffc
0x08048e32   mov dword ptr [ebp-0xbc], eax
0x08048e38   mov eax, dword ptr [ebp-0xf4]
0x08048e3e   add eax, 0x10
0x08048e41   mov dword ptr [ebp-0xf4], eax
0x08048e47   jmp 0x8049762
```

```
66
0x0804909b   mov eax, dword ptr [ebp-0xf4]
0x080490a1   add eax, 0x1
0x080490a4   mov dword ptr [ebp-0xf4], eax
0x080490aa   add esp, 0x1a0
0x080490b0   pop esi
0x080490b1   pop ebx
0x080490b2   pop ebp
0x080490b3   ret
```

```
67
0x08048892   jmp 0x8048897
0x08048897   mov eax, dword ptr [ebp-0xf8]
0x0804889d   sub eax, 0xd8
0x080488a2   mov dword ptr [ebp-0x180], eax
0x080488a8   jz 0x8048c75
0x08048c75   lea eax, ptr [ebp-0x34]
0x08048c78   mov ecx, dword ptr [ebp-0xf4]
0x08048c7e   add ecx, 0x1
0x08048c81   mov dword ptr [ebp-0xf4], ecx
0x08048c87   mov ecx, dword ptr [ebp-0xbc]
0x08048c8d   mov ecx, dword ptr [ecx]
0x08048c8f   mov edx, dword ptr [ebp-0xf4]
0x08048c95   mov edx, dword ptr [edx]
0x08048c97   mov edx, dword ptr [ebp+edx*4-0xf0]
0x08048c9e   mov ecx, dword ptr [ecx+edx*1]
0x08048ca1   mov edx, dword ptr [ebp-0xf4]
0x08048ca7   mov edx, dword ptr [edx+0x4]
0x08048caa   mov dword ptr [ebp+edx*4-0xf0], ecx
0x08048cb1   mov ecx, dword ptr [ebp-0xf4]
0x08048cb7   add eax, dword ptr [ecx+0xc]
0x08048cba   mov ecx, dword ptr [ebp-0xf4]
0x08048cc0   mov ecx, dword ptr [ecx+0x10]
0x08048cc3   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08048cca   mov eax, dword ptr [ebp-0xf4]
0x08048cd0   mov eax, dword ptr [eax+0x8]
0x08048cd3   mov eax, dword ptr [ebp+eax*4-0xf0]
0x08048cda   mov ecx, dword ptr [ebp-0xf4]
0x08048ce0   mov ecx, dword ptr [ecx+0x14]
0x08048ce3   mov ecx, dword ptr [ebp+ecx*4-0xf0]
0x08048cea   mov dword ptr [ecx], eax
0x08048cec   mov eax, dword ptr [ebp-0xbc]
0x08048cf2   add eax, 0xfffffffc
0x08048cf5   mov dword ptr [ebp-0xbc], eax
0x08048cfb   mov eax, dword ptr [ebp-0xf4]
0x08048d01   add eax, 0x18
0x08048d04   mov dword ptr [ebp-0xf4], eax
0x08048d0a   jmp 0x8049762
```

```
68
0x080493a9   lea eax, ptr [ebp-0x34]
0x080493ac   mov ecx, dword ptr [ebp-0xf4]
0x080493b2   add ecx, 0x1
0x080493b5   mov dword ptr [ebp-0xf4], ecx
0x080493bb   mov ecx, dword ptr [ebp-0xbc]
0x080493c1   mov ecx, dword ptr [ecx]
0x080493c3   mov ecx, dword ptr [ecx]
0x080493c5   mov edx, dword ptr [ebp-0xf4]
0x080493cb   mov edx, dword ptr [edx]
0x080493cd   mov dword ptr [ebp+edx*4-0xf0], ecx
0x080493d4   mov ecx, dword ptr [ebp-0xf4]
0x080493da   add eax, dword ptr [ecx+0x4]
0x080493dd   mov ecx, dword ptr [ebp-0xf4]
0x080493e3   mov ecx, dword ptr [ecx+0x8]
0x080493e6   mov dword ptr [ebp+ecx*4-0xf0], eax
0x080493ed   mov eax, dword ptr [ebp-0xf4]
0x080493f3   mov eax, dword ptr [eax+0x10]
0x080493f6   mov eax, dword ptr [ebp+eax*4-0xf0]
0x080493fd   mov ecx, dword ptr [ebp-0xf4]
0x08049403   mov ecx, dword ptr [ecx+0xc]
0x08049406   mov ecx, dword ptr [ebp+ecx*4-0xf0]
0x0804940d   mov dword ptr [ecx], eax
0x0804940f   mov eax, dword ptr [ebp-0xf4]
0x08049415   mov eax, dword ptr [eax+0x18]
0x08049418   mov ecx, dword ptr [ebp-0xf4]
0x0804941e   mov ecx, dword ptr [ecx+0x14]
0x08049421   mov dword ptr [ebp+ecx*4-0xf0], eax
0x08049428   mov eax, dword ptr [ebp-0xbc]
0x0804942e   add eax, 0xfffffffc
0x08049431   mov dword ptr [ebp-0xbc], eax
0x08049437   mov eax, dword ptr [ebp-0xf4]
0x0804943d   add eax, 0x1c
0x08049440   mov dword ptr [ebp-0xf4], eax
0x08049446   jmp 0x8049762
```